in the document or information, foreign government information incorporated in DoD documents shall be identified in a manner that ensures that such information is not declassified prematurely or made accessible to nationals of a third country without consent of the originator. This requirement may be satisfied by marking the face of the document ''FOREIGN GOVERNMENT INFORMATION,'' or with another marking that otherwise indicates that the information is foreign government information, and by including the appropriate identification in the portion or paragraph classification markings, for example, (NS) or (U.K.–C). All other markings prescribed by §159a.31(d) are applicable to these documents. In addition, DoD classified documents that contain extracts of NATO classified information shall bear a marking substantially as follows on the cover or first page: ''THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION.''

(2) When foreign RESTRICTED or NATO RESTRICTED information is included in an otherwise unclassified DoD document, the DoD document shall be marked CONFIDENTIAL. All requirements of §159a.31(d) apply to such documents. Portion markings on such a document include, for example ''(U),'' ''(NR),'' and ''(FRG–R).'' In addition, the appropriate caveat from paragraph (a) of this section, shall be included on the face of the document.

(3) The ''Classified by'' line of DoD documents containing only foreign government information normally shall be completed with the identity of the foreign government or international organization involved, for example, ''Classified by Government of Australia'' or ''Classfied by NATO,'' provided that other requirements of §159a.31(e) do not pertain to such documents.

(4) The ''Declassify on'' line of DoD documents containing foreign government information normally shall be completed with the notation ''Originating Agency's Determination Required'' or ''OADR'' (see §159a.36 and §159a.75(b)).

§159a.78 Protective measures.

(a) *NATO Classified Information.* NATO classified information shall be safeguarded in accordance with the provisions of DoD Directive 5100.55.

(b) *Other Foreign Government Information.* (1) Classified foreign government information other than NATO information shall be protected as is prescribed by this part for U.S. classified information of a comparable classification.

(2) Foreign government information, unless it is NATO information, that is marked under §159a.77(c)(2) or §159a.77(e)(2) shall be protected as U.S. CONFIDENTIAL, except that such information may be stored in locked filing cabinets, desks, or other similar closed spaces that will prevent access by unauthorized persons.

Subpart M—Special Access Programs

§159a.80 Policy.

It is the policy of the Department of Defense to use the security classification categories and the applicable sections of E.O. 12356 and its implementing ISOO Directive, to limit access to classified information on a ''need-to-know'' basis to personnel who have been determined to be trustworthy. It is further policy to apply the ''need-to-know'' principle in the regular system so that there will be no need to resort to formal Special Access Programs. Also, need-to-know control principles shall be applied within Special Access Programs. In this context, Special Access Programs may be created or continued only on specific showing that:

(a) Normal management and safeguarding procedures are not sufficient to limit ''need-to-know'' or access; and

(b) The number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information invoved.

§159a.81 Establishment of special access programs.

(a) Procedures for the establishment of Special Access Programs involving NATO classified information are based

on international treaty requirements (see DoD Directive 5100.55).

(b) The policies and procedures for access to and dissemination of Restricted Data and Critical Nuclear Weapon Design Information are contained in DoD Directive 5210.2.

(c) Special Access Programs for foreign intelligence information under the cognizance of the Director of Central Intelligence, or those of the National Telecommunications and Information Systems Security Committee originate outside the Department of Defense. However, coordination with the DUSD(P) and the Component's central point of contact is necessary before the establishment or implementation of any such Programs by any DoD Component. The information required by §159a.80(f)(1) will be provided.

(d) Excluding those Programs and that information specified in paragraphs (a)(1), (2), and (3) of this section, Special Access Programs shall be established within the Military Departments by:

(1) Submitting to the Secretary of the Department the information required under §159a.80(f)(1).

(2) Obtaining written approval from the Secretary of the Department;

(3) Providing to the DUSD(P) notice of the approval; and

(4) Maintaining the information and rationale upon which approval was granted within the Military Department's central office.

(e) Excluding those Programs and that information in paragraphs (d)(1), (2), and (3) of this section, Special Access Programs that are desired to be established in any DoD Component other than the Military Departments shall be submitted with the information referred to in §159a.80(f)(1) to the DUSD(P) for approval.

(f) Upon specific written notice to one of the appropriate DoD Special Access Program approval officials, receipt of their written concurrence, protective Special Access Program controls may be applied to a prospective Special Access Program for up to a 6-month period from the date of such notice. However, in all instances, the Program must be terminated as a prospective Special Access Program or formally approved as a Special Access Program by the end of the 6-month time period.

(g) Unless under DoD Directive S–5210.36[37], Special Access Programs which involve one or more DoD Components, or a DoD Component and a non-DoD activity, shall be covered by a written agreement which must document who has the principal security responsibility, who is the primary sponsor of the Program, and who is responsible for obtaining Special Access Program approval.

§159a.82 Review of special access programs.

(a) Excluding those Programs specified in §159a.81 (a), (b), or (c), each Special Access Program shall be reviewed annually by the DoD Component responsible for establishment of the Program. To accommodate such reviews, DoD Components shall institute procedures to ensure the conduct of annual security inspections, with or without prior notice, and regularly scheduled audits by security, contract administration, and audit organizations. Also, Program managers shall ensure that Special Access Program activities have undergone a current review by legal counsel for compliance with law, executive order, regulation, and national policy. To accomplish such reviews, specially cleared pools of attorneys may be utilized, but in all cases legal counsel shall be provided with all information necessary to perform such reviews.

(b) Special Access Programs, excluding those specified in §159a.81 (a), (b), or (c), or those required by treaty or international agreement, shall terminate automatically every 5 years unless reestablished in accordance with the procedures contained in §159a.81.

§159a.83 Control and central office administration.

(a) Special Access Programs shall be controlled and managed in accordance with DoD Directive 5205.7[38]. Each DoD Component shall appoint a Special Access Program coordinator to establish and maintain a central office and to serve as a single point of contact for

[37] See footnote 13 to §159a.33(j).

[38] See footnote 1 to §159a.3.